IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Liqun Chen, Keith A. Harrison, and David Soldera		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Method and Apparatus for Use in Relation to Verifying an Association Between Two Parties		
Serial No.:	10/613,522	Confirmation No.	4783
Examiner:	Shanto Abedin	Group Art Unit:	2436
Docket No.:	300202699-3	Filing Date:	July 2, 2003

May 18, 2009

Mail Stop APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 1.191

Dear Sir:

Appellants submit this Appeal Brief pursuant to the Notice of Appeal filed in the above-identified patent application on March 16, 2009. Appellants submit that this Appeal Brief is being timely filed, but if an extension of time is required for timely filing of this Appeal Brief, an extension of time is hereby requested. Authorization for payment of the fees required for acceptance of this Appeal Brie is provided in an accompanying transmittal letter.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, L.P., as named in the caption above. Hewlett-Packard Development Company, L.P., is a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA.

PATENT LAW OFFICE OF DAVID MILLERS
1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667
PH: (530) 621-4545
FX: (530) 621-4543

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no pending appeals, interferences or

judicial proceedings and no prior interferences or judicial proceedings known to Appellant, the Appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal. A prior appeal to the Board of a Final Office Action dated September 20, 2007 in the above-identified patent application included a Notice of Appeal submitted December 20, 2007 and a "Brief on Appeal (Amended)" submitted April 6, 2008. The prior appeal resulted in withdrawal of the Final Office Action dated September 20, 2007 and issuance of the Non-Final Office Action dated June 18, 2008.

III. STATUS OF CLAIMS

Claims 1-11, 19-24, and 29 are pending in the above-identified patent application and appear in an Appendix below. Claims 12-18 and 25-28 have been canceled. Claims 8-11 were indicated as being allowable in the Final Office Action dated December 15, 2009, and claims 6 and 7 were objected to but indicated allowable if amended to independent form including the limitations of their respective base claims and any intervening claims. Claims 1-7 and 19-21 were objected to based on informalities, but the objection to claims 1-7 and 19-21 was withdrawn in view of Appellants' after-final amendment dated February 24, 2009. Claims 1-5, 19-24, and 29 stand rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

There are no unentered amendments in this case. Appellants submitted an after-final amendment on February 24, 2009, and the Advisory Action dated March 11, 2009 indicated that the amendment would be entered for the purpose of appeal. The Claim Appendix below lists the claims as amended by Appellants on February 24, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed invention generally relates to enabling a third party to verify the existence of an association (any type of association) between a first party and a second party and involves the second party outputting three verification parameters that the third party can use to verify the association. More specifically, the three parameters enable the third party to verify that the second party holds a secret that must have been provided by the first party (it is assumed that this secret would have been provided by the first party to the second party in order to enable the existence of an association between the first and second parties to be

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

proved); this secret is called a "shared secret" in claim 1 because it is a secret shared by the first party with the second party, though the first party need not, in fact, keep a copy of the secret.

Independent claim 1 is more specifically directed to a method of enabling a second party (page 9, lines 13-18; Fig. 2, element 6) to prove to a third party (page 9, lines 13-18; Fig. 2, element 7) the existence of an association between the second party and a first party (page 9, lines 13-18; Fig. 2, element 5), the first party being associated with a first element (page 10, l, 1- page 16, line 3; element P) of a first algebraic group (page 2, line 6 to page 3., line 16, element G1; page 15, lines 5-10), the second party being associated with a second element (page 13, line 27 - page 14, line 19; element QTA2), of a second algebraic group (page 2, line 6 to page 3, line 16, element G1), formed from an identifier string (page 14, line 1, TA2) of the second party (page 9, lines 13-18; Fig. 2, element 6) using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party: receives a shared secret (Table I; element s1QTA2) provided by the first party as the product of a first secret (page 10, lines 1-2; element s1) and the second element (page 13, line 27 - page 14, line 19; element QTA2); computes first (page 14, lines 8-19; element r•(s1QTA2)), second (page 14, lines 8-19; element r• (QTA2)) and third (page 14, lines 8-19; element r•(P)) verification parameters as the product of a second secret (page 14, line 14; element r) with said shared secret (Table I; element s1QTA2), the second element (page 13, line 27 - page 14, line 19; element QTA2) and the first element (page 10, l, 1- page 16, line 3; element P) respectively; and outputs the first (page 14, lines 8-19; element r•(s1QTA2)), second (page 14, lines 8-19; element r• (QTA2)) and third (page 14, lines 8-19; element r• (P)) verification parameters for use by the third party (page 9, lines 13-18; Fig. 2, element 7) in proving the association between the first (page 9, lines 13-18; Fig. 2, element 5) and second parties (page 9, lines 13-18; Fig. 2, element 6).

To reiterate, claim 1 concerns a "second-party computer entity" (page 9, lines 13-18; Fig. 2, element 6) generating and outputting three verification parameters (page 14, lines 8-19) of the following form:

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

a first verification parameter computed as the product of the second secret (r) with the shared secret (s1QTA2) ;

a second verification parameter computed as the product of the second secret (r) with the second element (page 13, line 27 - page 14, line 19; element QTA2);

a third verification parameter computed as the product of the second secret (r) with the first element (P).

Independent claim 8 is not subject to this appeal.

Independent claim 19 is directed to an apparatus arranged to enable a third party (page 9, lines 13-18; Fig. 2, element 7) to verify an association between the apparatus and a first party (page 9, lines 13-18; Fig. 2, element 5) that has a first secret (s1) and is associated with a first element (page 10, line 1 to page 16, line 3; element P) of a first algebraic group (page 2, line 6 to page 3, line 16, element G1), the apparatus being associated with a second element (page 13, line 27 - page 14, line 19; element QTA2), of a second algebraic group (page 2, line 6 to page 3, line 16, element G2), and the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

a memory for holding a second secret (page 14, line 14; element r) and an identifier string (page 14, line 1, TA2) associated with the apparatus,

means for forming said second element (page 13, line 27 - page 14, line 19; element QTA2) from said identifier string (page 14, line 1, TA2) using a hash function,

means for receiving from the first party a shared secret (s1P) based on said first secret (page 10, lines 1-2; element s1) and said first element (page 10, line 1 to page 16, line 3; element P), and for storing this shared secret in the memory,

means for computing first (page 14, lines 8-19; element r•(s1QTA2)), second (page 14, lines 8-19; element r•(QTA2)) and third (page 14, lines 8-19; element r•(P)) verification parameters as the product of the second secret with said shared secret, said second element and said first element respectively, and

means for making available said identifier string and said verification parameters to the third party (page 9, lines 13-18; Fig. 2, element 7).

Independent claim 22 is directed to an apparatus for verifying an association between a first party [page 9, lines 13-18; Fig. 2, element 5] associated with a first element [page 10, line 1 to page 16, line 3; element P], of a first algebraic group [page 2, line 6 to page 3., line 16, element G1], and a second party [page 9, lines 13-18; Fig. 2, element 6] associated with a second element [page 13, line 27 - page 14, line 19; element QTA2], of a second algebraic group [page 2, line 6 to page 3, line 16, element G2]; the first and second elements being such that there exists a bilinear mapping p [page 7, line 27 - page 8, line 13] for these elements; the apparatus comprising:

means for receiving both data indicative of the first element [page 10, line 1 to

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

page 16, line 3; element P], and a first product [s1P] formed by the first party from a first secret [page 10, lines 1-2; element s1] and the first element [page 10, line 1 to page 16, line 3; element P];

means for receiving in respect of the second party both an identifier string [page 14, line 1, TA2], and first [page 14, lines 8-19; element r•(s1QTA2)], second [page 14, lines 8-19; element r•(QTA2)] and third [page 14, lines 8-19; element r•(P)] verification parameters;

means for computing the second element from the identifier string of the second party using a hash function;

means for carrying out a first check:

p(third verification parameter [page 14, lines 8-19; element r•(P)], computed second element [QTA2])= p(first element [page 10, line 1 to page 16, line 3; element P], second verification parameter [page 14, lines 8-19; element r•(QTA2)])

means for carrying out a second check:

p(first element [page 10, line 1 to page 16, line 3; element P], first verification parameter [page 14, lines 8-19; element r•(s1QTA2)])= p(first product [s1P], second verification parameter [page 14, lines 8-19; element r•(QTA2)]);

means responsive to both checks being passed, to confirm that there exists an association between the first and second parties.

Independent claim 29 is directed to a method of enabling a second party (page 9, lines 13-18; Fig. 2, element 6) to prove to a third party (page 9, lines 13-18; Fig. 2, element 7) the existence of an association between the second party and a first party (page 9, lines 13-18; Fig. 2, element 5), the first party being associated with a first element (page 10, line 1 to page 16, line 3; element P) of a first algebraic group (page 2, line 6 to page 3, line 16, element G1; page 15, lines 5-10), the second party being associated with a second element (page 13, line 27 - page 14, line 19; element QTA2), of a second algebraic group (page 2, line 6 to page 3, line 16, element G1), formed from an identifier string (page 14, line 1,TA2) of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party:

(1) receives a shared secret (Table I; element s1QTA2) provided by the first party as the product of a first secret (page 10, lines 1-2; element s1) and the second element;

(2) computes:

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

(i) a first verification parameter (page 14, lines 8-19; element r•(s1QTA2)) as the product of a second secret with said shared secret,

(ii) a second verification parameter (page 14, lines 8-19; element r•(QTA2)) as the product of the second secret with the second element, and

(iii) a third verification parameter (page 14, lines 8-19; element r•(P))as the product of the second secret with the first element; and

(3) outputs the first, second and third verification parameters for use by the third party (page 9, lines 13-18; Fig. 2, element 7) in proving the association between the first and second parties.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellants seek review of the following grounds for rejections:

A. Claims 22-24 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

B. Claims 1-5, 19-21, and 29 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. App. Pub. No. 2003/0182554 (Gentry '554) in view of U.S. Pat. App. Pub. No. 2003/0081785 (Boneh) and further in view of U.S. Pat. App. Pub. No. 2003/0179885 (Gentry '885).

VII. ARGUMENT

A. Claims 22-24 are directed to statutory subject matter.

Independent claim 22 is an apparatus or machine claim containing elements that are expressed using mean-plus-function language. The Final Office Action in the paragraph bridging pages 3 and 4 indicates, "according to the specification (please see Par 0069 and 0117), all of the claimed "means for" can be optionally implemented in computer program or software alone. Therefore, claimed invention is considered to be non-statutory as being directed to a program per se product."

The rejection is in error because: 1) the specification does not disclose software per se for performing the recited functions but instead discloses functional systems and products; and 2) even if the specification did disclose software per se, claim 22 recites a machine and

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

interpreting mean-plus-function elements to cover non-statutory subject matter is improper, when statutory subject matter is disclosed for performing the functions called for in the claims.

The portions of the specification cited in this rejection are paragraph [0069], which begins on page 8, line 17 of Appellants' specification, and paragraph [0117], which begins on page 13, line 23 of Appellants' specification. Paragraph [0069] of Appellants' specification states, "The present invention also encompasses apparatus and computer program products both for providing verification parameters enabling verification of an association between two parties, and for carrying out a verification check using these parameters." Thus, Appellants' specification in paragraph [0069] refers to "computer program products," not to a computer program per se. Paragraph [0117] of Appellants' specification states, "The first, second, third and fourth computer entities 10, 20, 30, 40 are conventional program-controlled computing devices though specialised hardware may be provided to effect particular cryptographic processes." Paragraph [0117] thus refers to "program-controlled computing devices" and specialized hardware, both of which are clearly statutory subject matter under 35 U.S.C. § 101. Accordingly, to the extent that the paragraphs cited in this rejection define the means-plus-function elements recited in claim 22, the Examiner errs by interpreting Appellants' specification as providing a correlation between the means-plus-function elements of claim 22 and a computer program per se.

Appellants further submit that that the recited elements of claim 22 preclude interpretation of those elements as being a non-statutory "computer program" because claim 22 recites a machine, which is one of the classes of patentable subject matter specifically enumerated in 35 U.S.C. § 101. In general, "machine" claims having means elements may only be reasonably viewed as process claims if there is no supporting structure in the written description that corresponds to the claimed means elements. See State Street Bank & Trust Co. v. Signature Financial Group, Inc. 149 F.3d 1368. (Fed. Cir. 1998) and In re Alappat, 33 F.3d 1526, 1540-41, 31 USPQ2d 1545, 1554 (Fed.Cir.1994) (in banc). Appellants' specification contains very detailed process steps that when carried out by general purpose computers create specific machines implementing the means recited in claim 22. Further, the Examiner has not alleged that any mean elements are insufficiently disclosed, or that claim 22 was being treated as a process claim for the purpose of determining whether claim 22 contained statutory subject matter under 35 U.S.C. § 101.

For the above reasons, claim 22 recites statutory subject matter.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

Claims 23 and 24 depend from claim 22 and therefore inherit the statutory subject matter of claim 22.

B. Claims 1-5, 19-21, and 29 are patentable under 35 U.S.C. § 103(a) over U.S. Pat. App. Pub. No. 2003/0182554 (Gentry '554) in view of U.S. Pat. App. Pub. No. 2003/0081785 (Boneh) and further in view of U.S. Pat. App. Pub. No. 2003/0179885 (Gentry '885).

Independent claim 1 distinguishes over the combination of Gentry '554, Boneh, and Gentry '885 by reciting, "A method of enabling a second party to prove to a third party the existence of an association between the second party and a first party, … wherein a second-party computer entity, acting on behalf of the second party: … computes first, second and third verification parameters, wherein the first verification parameter is a product of a second secret and said shared secret, the second verification parameter is a product of the second secret and the second element and the third verification parameter is a product of the second secret and the first element; and outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties." The combination of Gentry '554, Boneh, and Gentry '885 fails to disclose or suggest use of three verification parameters as recited in claim 1.

In regard to computing and outputting three verification parameters, the Examiner cites Figs. 4 and 5 and paragraphs [0024] and [0025] of Gentry '554. Gentry '554 discloses a Private Key Generator (PKG) that has a secret **s** used to supply two entities A and B with respective secrets $\mathbf{S_A}$ (= $\mathbf{sP_A}$) and $\mathbf{S_B}$ (= $\mathbf{sP_B}$), where $\mathbf{P_A}$ and $\mathbf{P_B}$ are public elements formed from the identities of entities A and B respectively. See paragraph [0022] of Gentry '554. The two entities A and B can form a non-interactive shared secret $\mathbf{S_{AB}}$ by using bilinear mapping as is explained at line 14 of paragraph [0022] of Gentry '554. The entities A and B also form an interactive shared secret by the exchange of intermediate shared secret components. Thus, for the Fig. 5 embodiment, entity A which has a secret **a**, passes a value **aP** to entity B, whereas entity B, which has a secret **b**, passes a value **bP** to entity A. **P** is a public element. Both entities can now form **abP** as described in paragraph [0033] of Gentry '554. Entities A and B can then form a common symmetric key using at least the interactive shared secret. The formation of the symmetric key seems to be the purpose of the Gentry '554 arrangement, the symmetric key being used to secure communication between the

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

entities. See paragraph [0002] of Gentry '554.

The Final Office Action on page 5 appears to identify symmetric key value g^{ab} or **abP** as the first verification parameter, value g^{b} or **bP** as the second verification parameter, and value g^{a} or **aP** as the third verification parameter. (The first full paragraph of page 5 of the final rejection, which refers to the verification parameters of claim 1, is unclear, so Appellants request clarification if this interpretation is incorrect.)

In regard to first verification parameter, value **abP** is generated as the product of a secret **a** or **b** held by one entity A or B and an intermediate shared secret component **bP** or **aP** supplied by the other entity B or A. See paragraph [0033] of Gentry '554. Component **bP** is computed by one entity B as the product of secret **b** with public element **P**, and component **aP** is computed by the other entity A as the product of random secret **a** with public element **P**. The public element **P** is a factor of all three components **abP**, **bP**, and **aP** as is the second secret recited in claim 1, but **P** is a public element not a secret as required in claim 1. More specifically, the quantity **P** is the generator of the first group G (see paragraph [0020]) and is public (see paragraph [0033]) where P is described as " a public parameter from the first cyclic group G"). **P** would actually be published by the third-party private key generator PKG. Clearly, the public generator P cannot be equated to a secret held by the entity computing the verification parameters. If the second secret of claim 1 was, in fact, public, as is public parameter **P**, the verification parameters would be worthless.

Additionally, values **aP** and **bP** can only be computed by the distinct entities A and B respectively as only entity A knows secret **a** needed to compute component **aP** and only entity B knows secret **b** needed to compute the first intermediate shared secret component **bP**. However, claim 1 requires that "a second-party computer entity, acting on behalf of the second party" computes all three verification parameters.

Further, the second verification parameter of claim 1 is computed as the product of the second secret with the 'second element' where the latter is an element of a second algebraic group and is formed from an identifier string (e.g., "TA2") of the second party using a hash function. The Gentry '554 equivalent to the 'second element' of claim 1 may be either $\mathbf{P_A}$ or $\mathbf{P_B}$ (see paragraph [0022]) depending on whether entity A or B of Gentry is considered to correspond to the "second-party computer entity" of claim 1. The only quantities in Gentry '554 that are formed as the product of a secret with $\mathbf{P_A}$ or $\mathbf{P_B}$ (and are thus candidates for the second verification parameter) are $\mathbf{S_A}$ (=s$\mathbf{P_A}$) and $\mathbf{S_B}$ (= s$\mathbf{P_B}$). Again, see paragraph [0022]. However, neither $\mathbf{S_A}$ nor $\mathbf{S_B}$ can be the second verification parameter because:

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

S_A nor S_B are the private keys respectively of entity A and entity B (see paragraph [0022]). These private keys are kept secret by their respective entities A and B and are not output by these entities as required by claim 1; and

only the PKG of Gentry '554 can compute S_A nor S_B as it requires knowledge of the secret s which is only known to the PKG (see paragraph [0022]). However, the PKG of Gentry 554 is clearly not the "second-party computer entity" of claim 1, not least because it does not receive a shared secret from another entity as is required of the "second-party computer entity" of claim 1.

Accordingly, the Final Office Action by citing Gentry '554 as teaching or suggesting computing first, second and third verification parameters as recited in claim 1 fails to provide a prima facie justification for rejection of claim 1 under 35 U.S.C. § 103.

Furthermore, the failure of Gentry '554 to suggest the verification parameters recited by claim 1 is not addressed by combining Gentry '554 with Boneh and the Gentry '885, and the Examiner made no argument to this effect.

The Final Office Action acknowledges that Gentry '554 "fails to disclose expressly the first, second, and third verification parameters for use by the third party in proving the association between the first and second party." Boneh is cited as allegedly teaching authentication based on three indicia (parameter, master key and ID) that it would then be obvious to modify Gentry '554 in terms of the parameters the Examiner identified. However, there is no indication that the three values cited from Gentry '554 have anything to do with a third party verifying an association between first and second parties. Accordingly, it is unclear why such teaching from Boneh would be applicable to or be obvious to combine with Gentry '554.

35 U.S.C. § 103 "forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" KSR Int'l Co. v. Teleflex Inc., 127 S.Ct. 1727, 1734 (2007). The Court stated that obvious analysis "should be made explicit." Id. at 1740-41, citing In re Kahn, 441 F.3d 977,988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). For the reasons stated above, the Examiner has failed to provide the required articulated reasoning with some rational underpinning to support the legal

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

conclusion of obviousness.

Claims 2-5 depend from claim 1 and are patentable for at least the same reasons that claim 1 is patentable.

Independent claim 19 is patentable over the combination of Gentry '554, Boneh, and Gentry '885 at least for reciting, "means for computing first, second and third verification parameters, wherein the first verification parameter is a product of the second secret with said shared secret, the second verification parameter is a product of the second secret and said second element and the third verification parameter is a product of the second secret and said first element, and means for making available said identifier string and said verification parameters to the third party." For the same reasons given above in reference to claim 1, the combination of Gentry '554, Boneh, and Gentry '885 fails to disclose or suggest use of three verification parameters meeting the limitations of claim 19. Accordingly, claim 19 is patentable over Gentry '554, Boneh, and Gentry '885.

Claims 20 and 21 depend from claim 19 and are patentable for at least the same reasons that claim 19 is patentable.

Independent claim 29 is patentable over the combination of Gentry '554, Boneh, and Gentry '885 at least for reciting," A method of enabling a second party to prove to a third party the existence of an association between the second party and a first party, ... wherein a second-party computer entity, acting on behalf of the second party: ... (2) computes: (i) a first verification parameter as the product of a second secret with said shared secret, (ii) a second verification parameter as the product of the second secret with the second element, and (iii) a third verification parameter as the product of the second secret with the first element; and (3) outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties." For the same reasons given above in reference to claim 29, the combination of Gentry '554, Boneh, and Gentry '885 fails to disclose or suggest computing or use of three verification parameters meeting the limitations of claim 29. Accordingly, claim 29 is patentable over Gentry '554, Boneh, and Gentry '885.

Claims 1-5, 19-21, and 29 are thus patentable under 35 U.S.C. § 103(a) over U.S. Pat. App. Pub. No. 2003/0182554 (Gentry '554) in view of U.S. Pat. App. Pub. No. 2003/0081785 (Boneh) and further in view of U.S. Pat. App. Pub. No. 2003/0179885 (Gentry '885).

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

For the above reasons, Appellants submit the pending rejections in the Final Office Action are unfounded and request that the rejections of claims 1-5, 19-24, and 29 be reversed.

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this Appeal Brief or the application generally.

Respectfully submitted,

/David Millers 37396/

David Miller
Reg. No. 37,396

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

VIII. CLAIMS APPENDIX

Pending claims 1-11, 19-24, and 29 including claims 1-5, 19-24, and 29, which are the claims involved in this appeal, are copied below.

1. (Previously Presented) A method of enabling a second party to prove to a third party the existence of an association between the second party and a first party, the first party being associated with a first element of a first algebraic group, the second party being associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party:

receives a shared secret provided by the first party as the product of a first secret and the second element;

computes first, second and third verification parameters, wherein the first verification parameter is a product of a second secret and said shared secret, the second verification parameter is a product of the second secret and the second element and the third verification parameter is a product of the second secret and the first element; and

outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties.

2. (Previously Presented) A method according to claim 1, wherein the second-party computer entity generates a further shared secret from the second secret and an identifier string of a fourth party, the second party outputting this further shared secret to the fourth party for use by the latter as the private key of a public/private key pair the public key of which is formed by the identifier string of the fourth party.

3. (Original) A method according to claim 1, wherein the first and second parties are respectively parent and child trusted authorities in a hierarchy of trusted authorities.

4. (Original) A method according to claim 1, wherein the first and second algebraic groups are the same.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

5. (Original) A method according to claim 1, wherein the first and second elements are points on the same elliptic curve.

6. (Previously Presented) A method of verifying an association between the first and second parties of claim 1 by using a function p providing said bilinear map; the method comprising a third-party computer entity carrying out the following operations using the verification parameters of claim 1:

computing the second element from the identifier string of the second party;

carrying out a first check to determine that the following equality is satisfied:

p(third verification parameter, computed second element)

$= p$(first element, second verification parameter)

carrying out a second check to determine that the following equality is satisfied:

p(first element, first verification parameter)

$= p$(first product, second verification parameter) where said first product is a public parameter provided by the first party and corresponds to the product of the first secret and the first element;

verifying the existence of the association between the first and second parties only where checks are passed.

7. (Original) A method according to claim 6, wherein said bilinear mapping function is based on a Tate or Weil pairing.

8. (Previously Presented) A method of verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group, the first and second elements being such that there exists a bilinear mapping p for these elements, the method comprising a third-party computer entity carrying out the following operations:

receiving both data indicative of said first element, and a first product formed by the first party from a first secret and the first element;

receiving in respect of the second party an identifier string and first, second and third verification parameters;

computing the second element from the identifier string of the second party;

carrying out a first check to determine that the following equality is satisfied:

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

p(third verification parameter, computed second element) = p(first element, second verification parameter)

carrying out a second check to determine that the following equality is satisfied:

p(first element, first verification parameter)= p(first product, second verification parameter)

verifying the existence of the association between the first and second parties only where checks are passed.

9. (Original) A method according to claim 8, wherein said bilinear mapping function is based on a Tate or Weil pairing.

10. (Original) A method according to claim 8, wherein the first and second algebraic groups are the same.

11. (Original) A method according to claim 8, wherein the first and second elements are points on the same elliptic curve.

Claims 12 - 18. (Cancelled)

19. (Previously Presented) Apparatus arranged to enable a third party to verify an association between the apparatus and a first party that has a first secret and is associated with a first element of a first algebraic group, the apparatus being associated with a second element, of a second algebraic group, and the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

a memory for holding a second secret and an identifier string associated with the apparatus,

means for forming said second element from said identifier string using a hash function,

means for receiving from the first party a shared secret based on said first secret and said first element, and for storing this shared secret in the memory,

means for computing first, second and third verification parameters, wherein the first verification parameter is a product of the second secret with said shared secret, the second

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

verification parameter is a product of the second secret and said second element and the third verification parameter is a product of the second secret and said first element, and

means for making available said identifier string and said verification parameters to the third party.

20. (Original) Apparatus according to claim 19, wherein the first and second algebraic groups are the same.

21. (Original) A method according to claim 19, wherein the first and second elements are points on the same elliptic curve.

22. (Previously Presented) Apparatus for verifying an association between a first party associated with a first element, of a first algebraic group, and a second party associated with a second element, of a second algebraic group; the first and second elements being such that there exists a bilinear mapping p for these elements; the apparatus comprising:

means for receiving both data indicative of the first element, and a first product formed by the first party from a first secret and the first element;

means for receiving in respect of the second party both an identifier string, and first, second and third verification parameters;

means for computing the second element from the identifier string of the second party using a hash function;

means for carrying out a first check to determine that the following equality is satisfied:

p(third verification parameter, computed second element) = p(first element, second verification parameter);

means for carrying out a second check to determine that the following equality is satisfied:

p(first element, first verification parameter) = p(first product, second verification parameter);

means responsive to both checks being passed, to confirm that there exists an association between the first and second parties.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

23. (Original) Apparatus according to claim 22, wherein said bilinear mapping p is based on a Tate or Weil pairing.

24. (Original) Apparatus according to claim 22, wherein the first and second elements are points on the same elliptic curve.

Claims 25–28 (Cancelled)

29. (Previously Presented) A method of enabling a second party to prove to a third party the existence of an association between the second party and a first party, the first party being associated with a first element of a first algebraic group, the second party being associated with a second element, of a second algebraic group, formed from an identifier string of the second party using a hash function, and there being a computable bilinear map for the first and second elements; wherein a second-party computer entity, acting on behalf of the second party:

(1) receives a shared secret provided by the first party as the product of a first secret and the second element;

(2) computes:

(i) a first verification parameter as the product of a second secret with said shared secret,

(ii) a second verification parameter as the product of the second secret with the second element, and

(iii) a third verification parameter as the product of the second secret with the first element; and

(3) outputs the first, second and third verification parameters for use by the third party in proving the association between the first and second parties.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

IX. EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner that Appellant is relying upon in this appeal. In particular, Appellants' Declaration of Prior Invention, which was submitted with the Response to the Final Office Action dated February 24, 2009, was not entered by the Examiner and is not relied on in this Appeal Brief.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

X. RELATED PROCEDINGS APPENDIX

No decisions rendered by a court or the Board of Patent Appeals and Interferences are being submitted.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543